

## Configuration d'un serveur Apache2

<b>Savoirs</b>	<ul style="list-style-type: none"> <li>• Principes d'architecture d'un service (architecture du service Web) ;</li> <li>• Protocoles associés au service WEB : http, https ;</li> <li>• Chiffrement et certificat ;</li> <li>• Le protocole HTTPS et service Web sécurisé ;</li> </ul>
<b>Savoir-faire</b>	<ul style="list-style-type: none"> <li>• Caractériser un service et le serveur associé</li> <li>• Exploiter les fonctions de base d'un langage de commandes</li> <li>• Installer, configurer et administrer un service</li> <li>• Mettre en œuvre un protocole sécurisé associé à un service</li> </ul>
<b>Outils</b>	<p>Serveur Linux Debian.</p> <p><b>Serveurs/service</b> : apache2</p> <p><b>Clients</b> : navigateur web sur STA Linux, Windows ou autre système.</p> <p>Outils de capture et d'analyse de trames (Wireshark)</p>
<b>Mots-clés</b>	Service, dns, url, web, http, https, chiffrement, certificat

**Important** : Ajouter et commenter les copies d'écran des résultats des commandes exécutées.

### Etape 1 : Manipulations diverses

1. Installer les paquets `apache2` et `libapache2-mod-php` :

2. Avant de commencer à modifier la configuration, faites une sauvegarde du répertoire contenant la configuration d'apache : `/etc/apache2` :

```
root@Ch2Lab1:/home/centrecallbd# cp -r /etc/apache2 /etc/apache2.ori
root@Ch2Lab1:/home/centrecallbd# ls /etc/apache2.ori
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
```

3. Exécuter et expliquer le résultat de la commande suivante :

```
grep -ni "listen" /etc/apache2/ports.conf
```

```
root@Ch2Lab1:/home/centrecallbd# grep -ni "listen" /etc/apache2/ports.conf
5:Listen 80
8:      Listen 443
12:     Listen 443
```

**La commande permet de voir sur quel port on est.**

**Que fait la commande *grep* ?**

La commande *grep* permet de trouver un mot que l'on cherche.

**4. Exécuter et expliquer le résultat de la commande suivante :**

```
grep -nir "documentroot" /etc/apache2/*
```

```
root@Ch2Lab1:/home/centrecallbd# grep -nir "documentroot" /etc/apache2/*
/etc/apache2/sites-available/default-ssl.conf:5:          DocumentRoot /var/www/html
/etc/apache2/sites-available/000-default.conf:12:         DocumentRoot /opt
```

L'option « *r* » permet une recherche récursive dans les dossiers et sous-dossiers.

**Rappel :** La **configuration d'Apache** (comme celle de la plupart des services sur Linux) est **modulaire** c'est à dire que le fichier principal de configuration inclut des fichiers de configuration « externalisés » ayant chacun un rôle bien précis ; de plus, lors d'une mise à jour ce fichier pourrait être modifié. Il est donc fortement **déconseillé de le modifier** mais plutôt d'intervenir sur les fichiers inclus dans « **apache2.conf** ».

A chaque modification ou ajout de fichier, vérifier la syntaxe en exécutant la commande :

```
apache2ctl configtest ou apache2ctl -t
```

**5. Exécuter et noter le résultat de la commande :**

```
apache2ctl configtest
```

```
root@Ch2Lab1:/home/centrecallbd# apache2ctl configtest
Syntax OK
```

**6. Exécuter et expliquer le résultat de la commande suivante :**

```
apache2ctl status
```

OU

```
systemctl status apache2
```

La commande permet de se renseigner sur la fonctionnalité du service.

**7. Exécuter et expliquer le résultat de la commande suivante :**

```
tail -f /var/log/apache2/error.log
```

La commande permet d'avoir accès aux logs des erreurs.

## Processus et variables

### 8. Exécuter et expliquer le résultat de la commande suivante :

```
ps -ef | grep apache
root@Ch2Lab1:/home/centrecallbd# ps -ef | grep apache
root      674      1   0 14:58 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  715     674   0 14:58 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  716     674   0 14:58 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  717     674   0 14:58 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  718     674   0 14:58 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  719     674   0 14:58 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  720     674   0 14:58 ?        00:00:00 /usr/sbin/apache2 -k start
root     2928    2755   0 15:20 ?        00:00:00 tail -f /var/log/apache2/error.log
root     3070    3060   0 15:26 pts/1    00:00:00 grep apache
```

Il existe plusieurs processus.

- Que fait la commande `ps` ?

La commande `ps` permet d'afficher un processus.

- Quel est le numéro du processus père lancé par l'utilisateur « root » ?

Le numéro est 674

- Quels sont les processus fils lancés par l'utilisateur système « www-data » ?

Les processus fils lancés sont www-data.

### 9. Dans le fichier de configuration principale d'Apache2, quelles sont les valeurs des directives :

- User ? www-data
- PidFile ? /var/run/apache2\$SUFFIX/apache2.pid

### 10. Consulter le fichier « /etc/apache2/envvars » : fichier contenant les variables d'environnement.

- Quelle est la valeur de la variable d'environnement « APACHE\_RUN\_USER » ?

La valeur de la variable est www-data.

- Quelle est la valeur de la variable d'environnement « APACHE\_RUN\_GROUP » ?

La valeur de la variable est www-data.

- Quelle est la valeur de la variable d'environnement « APACHE\_PID\_FILE » ?

La valeur de la variable est /var/run/apache2\$SUFFIX/apache2.pid

- Quelle est la valeur de la variable d'environnement « APACHE\_LOG\_DIR » ?

La valeur de la variable est `/var/log/apache2$SUFFIX`

- Consultez le fichier correspondant à la variable d'environnement « `APACHE_PID_FILE` » ; à quoi correspond le nombre inscrit ?

Le PID correspond au processus du root.

### La directive `ServerName` : (voir annexes)

- A quoi sert cette directive ? Dans quels fichiers se trouve-t-elle ?

Le `ServerName` est le nom du serveur qui devra être tapé dans la barre d'adresse du navigateur.

### Le port d'écoute :

- Quelle est la directive principale qui définit le ou les ports d'écoute ?

On utilise la directive `listen` pour définir les ports d'écoute.

- Modifiez ponctuellement ce port d'écoute (dans toutes les directives nécessaires) en le mettant à 888 et relancez le serveur Web.

- Quelle est l'URL que vous devez saisir pour accéder à votre serveur Web ?

`888@localhost`

- Revenez à un port d'écoute normal : 80.

### Divers

- Dans quel fichier se trouvent les modules disponibles, mais non chargés ? Affichez-les.

alias.load	echo.load	proxy_fdpass.load
allowmethods.load	env.load	proxy_ftp.conf
asis.load	expires.load	proxy_ftp.load
auth_basic.load	ext_filter.load	proxy_hcheck.load
auth_digest.load	file_cache.load	proxy_html.conf
auth_form.load	filter.load	proxy_html.load
authn_anon.load	headers.load	proxy_http2.load
authn_core.load	heartbeat.load	proxy_http.load
authn_dbd.load	heartmonitor.load	proxy.load
authn_dbm.load	http2.conf	proxy_scgi.load
authn_file.load	http2.load	proxy_uwsgi.load
authn_socache.load	ident.load	proxy_wstunnel.load
authnz_fcgi.load	imagemap.load	ratelimit.load
authnz_ldap.load	include.load	reflector.load
authz_core.load	info.conf	remoteip.load
authz_dbd.load	info.load	reqtimeout.conf
authz_dbm.load	lbmethod_bybusyness.load	reqtimeout.load
authz_groupfile.load	lbmethod_byrequests.load	request.load
authz_host.load	lbmethod_bytraffic.load	rewrite.load
authz_owner.load	lbmethod_heartbeat.load	sed.load
authz_user.load	ldap.conf	session_cookie.load
autoindex.conf	ldap.load	session_crypto.load
autoindex.load	log_debug.load	session_dbd.load
brotli.load	log_forensic.load	session.load
buffer.load	lua.load	setenvif.conf
cache_disk.conf	macro.load	setenvif.load
cache_disk.load	md.load	slotmem_plain.load
cache.load	mime.conf	slotmem_shm.load
cache_socache.load	mime.load	socache_dbm.load
cern_meta.load	mime_magic.conf	socache_memcache.load
cgid.conf	mime_magic.load	socache_shmcb.load
cgid.load	mpm_event.conf	speling.load
cgi.load	mpm_event.load	ssl.conf
charset_lite.load	mpm_prefork.conf	ssl.load
data.load	mpm_prefork.load	status.conf
dav_fs.conf	mpm_worker.conf	status.load
dav_fs.load	mpm_worker.load	substitute.load
dav.load	negotiation.conf	suexec.load
dav_lock.load	negotiation.load	unique_id.load
dbd.load	php7.3.conf	userdir.conf
deflate.conf	php7.3.load	userdir.load
deflate.load	proxy_ajp.load	usertrack.load
dialup.load	proxy_balancer.conf	vhost_alias.load
dir.conf	proxy_balancer.load	xml2enc.load

Les modules se trouvent dans le fichier mods-available

- Dans quel fichier se trouvent les modules actifs sur votre serveur ? Affichez-les.

Les modules actifs sont dans le fichier mods-enabled

access_compat.load	authn_core.load	authz_user.load	deflate.load	dnssd.load	mime.load	negotiation.load	reqtimeout.load	status.load
alias.conf	authn_file.load	autoindex.conf	dir.conf	env.load	mpm_prefork.conf	php7.3.conf	setenvif.conf	
alias.load	authz_core.load	autoindex.load	dir.load	filter.load	mpm_prefork.load	php7.3.load	setenvif.load	
auth_basic.load	authz_host.load	deflate.conf	dnssd.conf	mime.conf	negotiation.conf	reqtimeout.conf	status.conf	

- Dans quel fichier se trouve la liste des sites disponibles ? Affichez-les.

Les sites disponibles se trouvent dans sites-available

000-default.conf	default-ssl.conf
------------------	------------------

- Dans quel fichier se trouve la liste des sites actifs ? Affichez-les.

Les sites actifs sont dans le dossier sites-enabled

000-default.conf

## Etape 2 : Création des Hôtes Virtuels (VHost)

### 1. Analyse de la configuration du site web par défaut

➤ Quel est le fichier représentant le site par défaut ? Donner son emplacement.

Le fichier représentant le site par défaut est dans /etc/apache2/sites-available et dans le fichier 000-default.conf

➤ Ouvrir le fichier de configuration du site par défaut et expliquer son contenu :

- <VirtualHost \* : 80> :
- ServerName : webmaster@localhost
- DocumentRoot : /opt
- ErrorLog : \${APACHE\_LOG\_DIR}/error.log
- Donner le chemin du dossier qui contient les pages du site par défaut. Afficher son contenu : /etc/apache2/sites-available 000-default.conf

```
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /opt

<Directory /opt>
Options Indexes FollowSymLinks
AllowOverride none
Require all granted
</Directory>

# Available loglevels: trace8, ..., tracel, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

- Quelle est la page web du site par défaut ? Afficher son contenu et donner son chemin :

```
root@Ch2Lab1:/var/www/html# ls
La page web du site par défaut est index.html
```

Son chemin est /var/www/html

- Donner le chemin du fichier qui stocke les logs liés aux erreurs. Afficher ce fichier.
- Donner le chemin du fichier qui stocke l'historique des accès au site. Afficher ce fichier.

## 2. Création et configuration d'un hôte virtuel (vhost)

Il est très courant d'héberger et de gérer plusieurs sites, dits "**virtuels**" (vhost), par un seul et même serveur (**hébergement mutualisé**).

**Ceux-ci sont appelés par les clients sous différents noms DNS** ; le serveur écoute une seule adresse IP à laquelle sont associés plusieurs noms de sites qui seront utilisés dans les URL clientes.

Les sociétés se partageant un serveur Web peuvent ainsi avoir leurs propres domaines accessibles.

### a. Création d'hôtes virtuels

- En vous basant sur le site par défaut, ajouter 2 hôtes virtuels pour les sites **sio1.local** et **sio2.local**.

**Important** : Les pages Web de chaque site seront placées dans les dossiers suivants :

- **/var/www/sio1/** : pour le site **sio1.local**.
- **/var/www/sio2/** : pour le site **sio2.local**.

- Activer ces 2 sites : **a2ensite ...**
- Tester avec un navigateur en utilisant l'adresse IP du serveur.
- Tester avec un navigateur en utilisant les noms de domaines **sio1.local** et **sio2.local**. Que remarquez-vous ? Quelles sont les solutions ?

- Pour les tests sur le serveur, configurer le fichier **/etc/hosts** en y ajoutant :

127.0.0.1	sio1.local	sio2.local	...
-----------	------------	------------	-----

- Pour les tests à partir d'un autre poste Linux configurer le fichier **/etc/hosts** en y ajoutant :

Adresse-ip-serveur	sio1.local	sio2.local	...
--------------------	------------	------------	-----

**Remarque** : le fichier hosts est l'ancêtre du système DNS. Il permet la résolution de noms de domaines en adresses IP. Ce fichier est présent dans la plupart des systèmes. Sur le système Windows, l'emplacement est : **C:\Windows\System32\drivers\etc\hosts**.

- Sur votre PC Windows, consulter ce fichier et noter son contenu.

**Important** : pour pouvoir le modifier, il faut l'ouvrir en tant qu'administrateur.

## b. L'accès sécurisé au serveur Web (https)

- Vérifiez si les paquetages « **openssl** » et « **libssl** » sont installés :

```
dpkg -l | grep libssl ou openssl
```

```
root@Ch2Lab1:/etc/apache2/sites-available# dpkg -l | grep libssl
ii libssl1.1:amd64 1.1.1n-0+deb10u6 amd64 Secure Sockets Layer toolkit - shared libraries
root@Ch2Lab1:/etc/apache2/sites-available# dpkg -l | grep openssl
ii openssl 1.1.1n-0+deb10u6 amd64 Secure Sockets Layer toolkit - cryptographic utility
ii perl-openssl-defaults:amd64 3 amd64 version compatibility baseline for Perl OpenSSL packages
```

### Configurer apache2 avec le module ssl

- Quel est le fichier représentant le site sécurisé par défaut ? Donner son chemin absolu.

Le fichier qui représente le site sécurisé par défaut est : `/etc/apache2/sites-available/default-ssl.conf`

- Ouvrir ce fichier et expliquer son contenu :
  - `<VirtualHost * : 443>` : Port d'écoute du VirtualHost
  - `SSLEngine on` : Le ssl est on
  - `SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem` : Chemin d'accès de la certification
  - `SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key` : Chemin d'accès de la clé
  - Afficher le contenu des 2 derniers fichiers.
- Activez le module « ssl » : `a2enmod ssl`
- Ajouter et configurer 2 hôtes virtuels pour les 2 sites Web sécurisés **sio1.local** et **sio2.local** : `sio1-ssl.conf` et `sio2-ssl.conf`
- Vérifier si votre serveur écoute sur le port 443 ou pas : `ss -nat | grep 443`.  
Afficher et expliquer le résultat :
- Tester à l'aide d'un navigateur : <https://localhost> ou <https://127.0.0.1> ou <https://votre-adresse-ip>. Que remarquez-vous ?

- Tester à l'aide d'un navigateur : <https://sio1.local> et <https://sio2.local>. Que remarquez-vous ?
- Renvoyer l'ensemble des requêtes HTTP vers le protocole HTTPS en ajoutant dans les fichiers de configuration des Vhosts la directive suivante :

```
<VirtualHost * : 80>
    ...
    Redirect / https://sio1.local
</VirtualHost>
```

- Vérifier en exécutant des requêtes <http://sio1.local> et <http://sio2.local>. Que constatez-vous ?

### 3. Analyse de l'activité du serveur Apache

- Taper la commande : **tail -f /var/log/apache2/access.log** et lancer une requête <http://sio1.local>. Que constatez-vous sur le terminal ?

On reçoit des logs de requête.

- Tester en effectuant une requête <https://sio1.local> et <https://sio2.local>. Que constatez-vous ?
- Tester en effectuant une requête vers la page <https://sio1.local/test.html>. Que constatez-vous ?
- Afficher le contenu du fichier **/var/log/apache2/error.log**. Que remarquez-vous ?

### 4. Analyse de trames

- Installer le capteur de trames Wireshark ;
- Capturer et analyser des trames à destination de votre serveur web Apache.

268	670.183328859	127.0.0.1	127.0.0.1	TCP	76	33030	-	80	[SYN]	Seq=0	Win=65495	Len=0	MSS=65495	SACK_PERM=1	TSval...
269	670.183337555	127.0.0.1	127.0.0.1	TCP	76	80	-	33030	[SYN, ACK]	Seq=0	Ack=1	Win=65483	Len=0	MSS=65495	SACK_P...
270	670.183344328	127.0.0.1	127.0.0.1	TCP	68	33030	-	80	[ACK]	Seq=1	Ack=1	Win=65536	Len=0	TSval=1182940404	TSec...
271	670.183393261	127.0.0.1	127.0.0.1	HTTP	514	GET / HTTP/1.1									
272	670.183401066	127.0.0.1	127.0.0.1	TCP	68	80	-	33030	[ACK]	Seq=1	Ack=447	Win=65152	Len=0	TSval=1182940404	TS...
273	670.183654698	127.0.0.1	127.0.0.1	HTTP	693	HTTP/1.1 200 OK (text/html)									
274	670.183659417	127.0.0.1	127.0.0.1	TCP	68	33030	-	80	[ACK]	Seq=447	Ack=626	Win=65024	Len=0	TSval=1182940404	...

```
- Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: sio2.local\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
  Accept-Language: fr-fr;q=0.9,en-US;q=0.5,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  If-Modified-Since: Thu, 01 Feb 2024 07:51:08 GMT\r\n
  If-None-Match: "17b-6104d422b0f5a-gzip"\r\n
  \r\n
  [Full request URI: http://sio2.local/]
  [HTTP request 1/1]
  [Response in frame: 273]
```

## 5. Hébergement du site Brocant'Art

- Créer un hôte virtuel pour l'hébergement du site Brocant'Art réalisé en AP du 1er semestre. Ce site sera accessible via le nom de domaine *www.brocant.fr*;
- Créer un dossier pour stocker les pages web du site ;
- Transférer les pages web vers votre serveur ;
  - Compresser le dossier contenant vos pages web ;
  - Transférer le dossier vers votre serveur Linux en utilisant la commande **scp** ;
  - Décompresser le dossier sur le serveur Linux ;
  - Déposer les pages web à la racine de l'hôte virtuel.
- Créer un hôte virtuel pour l'accès https ;
- Tester.

